Arbitrarily little knowledge can give a quantum advantage for nonlocal tasks

Jonathan Allcock,[1,*] Harry Buhrman,[2] and Noah Linden[1]

[1]Department of Mathematics, University of Bristol,
University Walk, Bristol BS8 1TW, United Kingdom
[2]CWI, Science Park 123, 1098 XG Amsterdam, The Netherlands

(Dated: 2nd March 2009)

It has previously been shown that quantum nonlocality offers no benefit over classical correlations for performing a distributed task known as nonlocal computation. This is where separated parties must compute the value of a function without individually learning anything about the inputs. We show that giving the parties some knowledge of the inputs, however small, is sufficient to "unlock"the power of quantum mechanics to out-perform classical mechanics. This role of information held locally gives new insight into the general question of when quantum nonlocality gives an advantage over classical physics. Our results also reveal a novel feature of the nonlocality embodied in the celebrated task of Clauser, Horne, Shimony and Holt.

Quantum theory allows for separated bodies to be correlated with one another more strongly than is achievable by any local classical means. Once viewed with suspicion, such correlations are now looked at as a valuable resource which enables certain tasks to be performed - including quantum cryptography [1], teleportation [2], dense-coding [3] and reducing communication complexity [4, 5] - which would otherwise be impossible classically. It is a fundamental question for quantum physics to characterise those tasks for which quantum resources offer a benefit over classical physics; this is the subject of this Letter.

Perhaps the most celebrated task for which quantum theory offers an advantage over classical mechanics is due to Clauser, Horne, Shimony and Holt (CHSH) [6]. In this task, Alice and Bob are spatially separated, and each possess a single particle. They are then each sent a uniformly random single input bit (z_1 and z_2 respectively), the value of which determines which of two measurements (with possible outcomes 0 or 1) they must perform on their particles. Conditioned on their measurement outcomes, Alice and Bob then each return a single bit (a and b respectively) with the aim of satisfying the following equation with as high a success probability as possible:

$$a \oplus b = AND(z_1, z_2) = z_1 z_2. \tag{1}$$

Thus, the output bit c of the AND function is the XOR of the two bits a and b, i.e. $c = a \oplus b$; this output is not known to Alice or Bob. As is well-known, if the particles are classical, the maximum success probability is 75%, but quantum correlations between the particles allow a success probability of $\sim 85\%$ to be achieved. Thus, quantum mechanics allows for greater success in solving this nonlocal task with the separated inputs z_1 and z_2. We will return to this fundamental example later, as we will see that previous work on it has missed an intriguing aspect of the nature of the inputs and outputs.

The task described above is asymmetric between the inputs and outputs in an important way: the output $c = a \oplus b$ is not known to Alice or Bob, whereas the inputs are. This led the authors of [7], following [8], to consider the situation where the input bits of a function are also distributed between Alice and Bob in such a way that neither has any knowledge of them: given an input bit z_j, Alice receives x_j and Bob y_j such that $z_j = x_j \oplus y_j$, and x_j and y_j are locally random, being with equal probability 0 or 1. This scenario is known as *nonlocal computation.* Surprisingly, it was found in [7] that quantum mechanics gives no benefit over classical mechanics for the nonlocal computation of any function $f(z_1, z_2, ..., z_n)$ of n bits. This result is simple and rather general. For example, it is true for any probability distribution on the input bits z_j and it does not matter how many parties the bits are distributed to; [7] also describes more general families of tasks for which quantum mechanics offers no advantage. This leads to the natural question as to whether this is the generic situation. Does quantum mechanics typically help for nonlocal tasks or not?

In this Letter we probe this question in the following way. In nonlocal computation, it is important that Alice and Bob individually know nothing about the inputs z_j. Here we consider that they are allowed a small amount of information about the inputs. By this we mean, for example, that rather than being totally uncorrelated with z_j, we allow x_j to have a probability $p \neq 1/2$ of being equal to z_j. We will show that for a series of tasks, even if p is arbitrarily close to (but not equal to) 1/2 , this small amount of knowledge "unlocks"the power of quantum mechanics to out-perform classical mechanics.

The plan of this Letter is as follows. Firstly, we consider the nonlocal AND of two bits and show explicitly how if Alice and Bob have an infinitesimal amount of knowledge of the input bits, then there are quantum strategies that out-perform any classical ones. We then give a family of functions with input sizes of increasing length for which the same is true. At the end of the letter we return to the CHSH task and argue that our results give new insight into the nonlocality it embodies.

Let us briefly review the concept of the nonlocal computation of a Boolean function $f : \{0,1\}^n \times \{0,1\}^n \to$

$\{0,1\}$ from $2n$ bits to a single bit [7]. This can be described as a particular kind of *nonlocal XOR game* [9] $G = (f, \pi)$ between a *verifier* V and two *provers*, Alice and Bob. In a general XOR game, the verifier selects a pair of n-bit strings $x = x_1 x_2 \ldots x_n$ and $y = y_1 y_2 \ldots y_n$ according to some joint probability distribution $\pi(x, y)$, and sends x to Alice and y to Bob. In response, Alice returns a single bit a to the verifier, and similarly Bob returns a single bit b. The verifier deems the computation of f to be successful if $a \oplus b = f(x, y)$, in which case Alice and Bob are said to win the game. Before the game commences, Alice and Bob (who know f) can meet to agree on a common strategy, but once the game has started they are forbidden from communicating with one another. The nonlocal computation of f corresponds to an XOR game where the following extra two conditions are imposed. Firstly, f cannot depend on x and y individually, but only on their bitwise XOR:

$$f(x, y) \equiv f(x \oplus y) \equiv f(z), \tag{2}$$

where $z = x \oplus y$ denotes the n-bit string $z = z_1 z_2 \ldots z_n$ where $z_i = x_i \oplus y_i$. The second requirement is that

$$\pi(x, y) = \frac{1}{2^n} \widetilde{p}(x \oplus y), \tag{3}$$

where $\widetilde{p}(x \oplus y) = \widetilde{p}(z)$ is an arbitrary probability distribution on $z = x \oplus y$. This ensures that neither Alice nor Bob has any knowledge about the inputs z_i of f, because regardless of the value of z_i, Alice and Bob receive bits x_i and y_i which are uniformly random.

Following [9] we define the *classical value* $\omega_C(G)$ of an XOR game $G = (f, \pi)$ to be the maximum probability with which Alice and Bob can win using purely classical (deterministic) strategies. Such a strategy corresponds to Alice and Bob choosing their output bits a and b to be functions of x and y respectively. It can be shown that $\omega_C(G) = \frac{1}{2}(1 + \varepsilon_C(G))$, where the *classical bias* ε_C is given by

$$\varepsilon_C(G) = \max \sum_{x,y} \pi(x, y)(-1)^{f(x,y)} A_x B_y, \tag{4}$$

and the maximum is taken over all $A_x, B_y \in \{-1, 1\}$. Note that ε_C is really twice the real bias of the success probability. Similarly we define the *quantum value* $\omega_Q(G)$ to be the maximum probability of successfully computing f when Alice and Bob utilize quantum strategies. Such strategies correspond to Alice and Bob sharing an entangled state $|\psi\rangle$ and, dependent on x and y, performing projective measurements on their respective subsystems corresponding to Hermitian operators a_x and b_y with eigenvalues 0 and 1. They then return their measurement results to the verifier. Analogously to the classical case, ω_Q can be expressed as $\omega_Q(G) = \frac{1}{2}(1 + \varepsilon_Q(G))$, where the *quantum bias* ε_Q has the form

$$\varepsilon_Q(G) = \max \sum_{x,y} \pi(x, y)(-1)^{f(x,y)} \langle\psi| A_x B_y |\psi\rangle ,$$

and the maximum is taken over all pure states $|\psi\rangle$ and Hermitian operators A_x and B_y (on Alice and Bob's subsystems respectively) with eigenvalues ± 1.

The surprising result of [7] is that there is no quantum advantage for the nonlocal computation of any function f. That is, when conditions (2) and (3) are imposed, $\omega_C(G) = \omega_Q(G)$, and quantum strategies do not allow the computation to succeed with higher probability than is classically possible. As an example consider the simplest interesting case, which we shall denote by G_{AND}. This is the game $G_{AND} = (f, \pi)$ where f is the 2-bit nonlocal AND function:

$$f(x \oplus y) = AND(z_1, z_2) = z_1 z_2, \tag{5}$$

where z is drawn according to the uniform distribution over two bits (i.e. $\pi(x, y) = (1/4)\widetilde{p}(z) = 1/16$). As shown in [7], the classical and quantum biases for this game are both equal to 1/2. However, suppose we relax condition (3), and allow Alice and Bob some local knowledge of the input bits z_i. For instance, suppose that Alice's bit x_1 has some probability p of being equal to z_1, and Bob's bit y_2 has some probability q of being equal to z_2. (Note that we still require $z_i = x_i \oplus y_i$.) Without loss of generality let us take $p, q \geq 1/2$. Denoting this new *perturbed game* by $G^{p,q}_{AND}$, the classical and quantum biases can be collectively expressed as:

$$\begin{aligned}\varepsilon_{C,Q}(G^{p,q}_{AND}) = \max \frac{1}{4}\mathbb{E}\,[&pqA_{00}B_{00} + pqA_{00}B_{01} + (1-p)qA_{00}B_{10} - (1-p)qA_{00}B_{11} \\ &+ p(1-q)A_{01}B_{00} + p(1-q)A_{01}B_{01} - (1-p)(1-q)A_{01}B_{10} + (1-p)(1-q)A_{01}B_{11} \\ &+ pqA_{10}B_{00} - pqA_{10}B_{01} + (1-p)qA_{10}B_{10} + (1-p)qA_{10}B_{11} \\ &- p(1-q)A_{11}B_{00} + p(1-q)A_{11}B_{01} + (1-p)(1-q)A_{11}B_{10} + (1-p)(1-q)A_{11}B_{11}] .\end{aligned} \tag{6}$$

Note that the case $p = q = 1/2$ is equivalent to the original game G_{AND} and has $\varepsilon_C(G_{AND}) = 1/2$ (c. f. equation 7). The case $p = q = 1$ corresponds to the standard CHSH task with $\varepsilon_C(G^{1,1}_{AND}) = 1/2$. A bit of thought shows that $\varepsilon_C(G^{p,q}_{AND})$ remains $1/2$, for any p and q. The reason is that the bias cannot *increase* when Alice and Bob have less information on z_1 and/or z_2. Any protocol for $G^{p,q}_{AND}$ $(p, q \geq 1/2)$ with bias b can be used to solve $G^{1,1}_{AND}$ with the same bias b as follows. Alice and Bob use two shared random bits r_1, r_2 such that $\Pr[r_1 = 0] = p$ and $\Pr[r_2 = 0] = q$. Alice uses $x_i \oplus r_i$ as her inputs to the protocol for $G^{p,q}_{AND}$ and Bob uses $y_i \oplus r_i$. It is easy to see that for these new inputs $\Pr[x_1 = z_1] = p$ and $\Pr[y_2 = z_2] = q$. A standard convexity argument shows that the above reduction can be massaged into a deterministic protocol. Hence the bias cannot increase for $p, q < 1$ and has to remain $1/2$.

On the other hand, by using quantum strategies Alice and Bob can do better. It is straightforward (although somewhat lengthy) to show that when $1 \geq (2q)^{-1} > p \geq 1/2$ (call this region 1),

$$\varepsilon_Q(G^{p,q}_{AND}) \leq \sqrt{q^2 + (1-q)^2}\sqrt{p^2 + (1-p)^2}, \qquad (7)$$

and when $1 \geq p \geq (2q)^{-1} \geq 1/2$ (call this region 2),

$$\varepsilon_Q(G^{p,q}_{AND}) \leq \frac{1}{\sqrt{2}}\left[1 - 2\left(1-p\right)\left(1-q\right)\right]. \qquad (8)$$

Note that the bounds (7) and (8) are strictly greater than $\varepsilon_C = 1/2$ for all values of p and q in the appropriate regions unless $p = q = 1/2$. Furthermore, there exist quantum strategies which attain these upper bounds. For region 1, Alice and Bob can share a maximally entangled state of four qubits (two for Alice and two for Bob) and choose measurement operators:

$$\begin{aligned}
&B_{00} = X \otimes I, \qquad B_{10} = (\cos\beta X + \sin\beta Z) \otimes I,\\
&B_{01} = Y \otimes X, \qquad B_{11} = -Y \otimes (\cos\beta X + \sin\beta Z),\\
&A_{00} = \left[p\left(\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} - \overline{B}_{11}\right)\right]/N_{00},\\
&A_{01} = \left[p\left(\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(-\overline{B}_{10} + \overline{B}_{11}\right)\right]/N_{10},\\
&A_{10} = \left[p\left(\overline{B}_{00} - \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} + \overline{B}_{11}\right)\right]/N_{10},\\
&A_{11} = \left[p\left(-\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} + \overline{B}_{11}\right)\right]/N_{11},
\end{aligned}$$

where $\cos\beta = \frac{1}{2}\frac{(p^2+(1-p)^2)(q^2+(1-q)^2)}{p(1-p)(q^2+(1-q)^2)}$, $N_{00} = N_{10} = 2q\sqrt{\frac{p^2+(1-p)^2}{q^2+(1-q)^2}}$, and $N_{01} = N_{11} = \frac{1-q}{q}N_{00}$. For region 2, an optimal strategy corresponds to Alice and Bob sharing a maximally entangled state of two qubits and choosing measurement operators:

$$\begin{aligned}
&B_{00} = B_{10} = X, \qquad B_{01} = -B_{11} = Z,\\
&A_{00} = \left[p\left(\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} - \overline{B}_{11}\right)\right]/M_{00},\\
&A_{01} = \left[p\left(\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(-\overline{B}_{10} + \overline{B}_{11}\right)\right]/M_{10},\\
&A_{10} = \left[p\left(\overline{B}_{00} - \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} + \overline{B}_{11}\right)\right]/M_{10},\\
&A_{11} = \left[p\left(-\overline{B}_{00} + \overline{B}_{01}\right) + (1-p)\left(\overline{B}_{10} + \overline{B}_{11}\right)\right]/M_{11},
\end{aligned}$$

where $M_{00} = M_{10} = \sqrt{2}$, and $M_{01} = M_{11} = \sqrt{2}(2p-1)$. Thus, if Alice and Bob have some knowledge about the input bits z_i (even an infinitesimal amount), quantum strategies do offer an advantage over classical strategies for computing the 2-bit nonlocal AND function.

We now show that there exists a family of games corresponding to functions with input sizes of increasing length for which the same is true. Underlying the game is a Boolean function $g : \{0,1\}^n \to \{0,1\}$. We partition the inputs $z = z_1, \ldots, z_n$ in two groups A and B, one for which Alice has some information, $\Pr[z_i = x_i] = p_i, i \in A$, and the rest for which Bob has some information, $\Pr[z_j = y_j] = p_j, j \in B$. For all i, $p_i \geq 1/2$. Each player thus has n inputs x_i, y_i. The distribution π over these inputs is specified as follows. The input z is distributed according to some distribution P. First pick z according to P, and then for $i \in B$ choose $x_i = z_i$ and $y_i = 0$ with probability p_i, and $x_i = 1 \oplus z_i$ and $y_i = 1$ with probability $1 - p_i$. Similarly for $j \in B$. Alice and Bob win the game iff $a \oplus b = g(x_1 \oplus y_1, \ldots, x_n \oplus y_n) = f(x, y)$. Note that the game satifies the no knowledge condition (3) when $p_i = q_i = 1/2$ for all i. We say that Alice or Bob have *some knowledge* of the game if not all p_i and q_i equal $1/2$.

Given any n-bit game $G_1 = (f_1, \pi_1)$ and any m-bit game $G_2 = (f_2, \pi_2)$, define their *sum* to be the game

$$G_1 \oplus G_2 = (f_1 \oplus f_2, \pi_1 \times \pi_2).$$

In this game, the verifier selects pairs of strings $\left((x^{(1)}, y^{(1)}), (x^{(2)}, y^{(2)})\right)$ according to the product distribution $\pi_1 \times \pi_2$. Alice and Bob win the game if on input $x^{(1)}, x^{(2)}$ and $y^{(1)}, y^{(2)}$, they output a and b such that $a \oplus b = f_1(x^{(1)}, y^{(1)}) \oplus f_2(x^{(2)}, y^{(2)})$. It was proved in [10] that the quantum bias of a sum of games is simply the product of the individual biases. This multiplicativity makes it easy to compute the quantum bias of a sum of games if the individual biases are known. Unfortunately it does not hold for the classical bias, which is in general MAXSNP hard to compute [11].

Now define the family of nonlocal distributed AND games by taking the k-fold sum of the game $G^{\frac{1}{2},\frac{1}{2}}_{AND}$.

$$G_{AND(k)} = \bigoplus_{j=1}^{k} G^{\frac{1}{2},\frac{1}{2}}_{AND}. \qquad (9)$$

By construction these games satisfy the 'no knowledge' condition (3), and hence there is no quantum advantage for any of them. Indeed, it follows from [10] that $\varepsilon_C(G_{AND(k)}) = \varepsilon_Q(G_{AND(k)}) = (1/2)^k$. As before, we can now consider allowing Alice and Bob some knowledge of the inputs, and define a family of perturbed games:

$$G^{p,q}_{AND(k)} = G_{AND(k-1)} \oplus G^{p,q}_{AND}. \qquad (10)$$

In other words, this is the family of games formed by taking the sum of $k-1$ copies of $G^{\frac{1}{2},\frac{1}{2}}_{AND}$ and a single copy of $G^{p,q}_{AND}$. We now show that for all k, there is a small region of (p,q)-space around $p=q=1/2$ in which a quantum advantage does exist. Fixing $q=1/2$, we allow p to vary in the interval $[1/2,1)$ (thus we remain in region 1). It follows from [10] and equation (7) that the quantum bias is

$$\varepsilon_Q(G^{p,1/2}_{AND(k)}) = \frac{1}{2^{k-1}\sqrt{2}}\sqrt{p^2+(1-p)^2}. \tag{11}$$

Observe that the success probability of *any* classical strategy will be a linear function in p, say $ap+b$, with a and b from a finite set of values. Moreover the quantum success probability equation (11) is monotone increasing for $p \geq 1/2$, and its derivative is 0 for $p=1/2$. Since for $p=1/2$ the quantum and the classical success probabilities are the same, and the classical value is always less than or equal to the quantum value, it follows that the line induced by the best classical protocol around $p=1/2$ is horizontal and not increasing. Thus, an infinitesimal amount of knowledge is sufficient for a quantum advantage to exist for this family of games. Indeed, it is clear from the construction of this example, that a quantum advantage also exists for any game $G = G_1 \oplus G^{p,1/2}_{AND}$, where G_1 has no quantum advantage and $p>1/2$.

Discussion. — We have shown that perturbing a nonlocal computation game by allowing Alice and Bob an arbitrarily small amount of local knowledge can be enough to give a quantum advantage over classical strategies.

Let us now make a few remarks. Firstly, as mentioned before, the bias of the game $G^{p,q}_{AND}$ for $p=q=1$ is equivalent to the standard CHSH expression (i.e. $\varepsilon_C = 1/2$, $\varepsilon_Q = 1/\sqrt{2}$). However the case $p=1$, $q=1/2$ is similar to the standard CHSH game, in that Alice has complete knowledge of her bit (i.e. $x_1 = z_1$). However, the second bit z_2 is completely unknown to Alice or Bob. Nonetheless, quantum protocols can do better than classical ones, and achieve the same value as in the true CHSH case. The CHSH scenario is usually understood as concerning the situation where Alice and Bob each have a bit locally and they output a bit: the output for the task being the XOR of the output bits. However the above observation shows that in fact equal success can be achieved in this task if, say, Alice knows one of the input bits, but neither Alice nor Bob have any knowledge of the other input bit; Bob can have no local information at all.

In this Letter we have focused on allowing Alice and Bob a particular kind of knowledge of the inputs of f. In fact, more general perturbations can be considered by relaxing the 'no knowledge' condition (3) completely, and allowing the probability distribution $\pi(x,y)$ to be arbitrary. Then, given a game $G=(f,\pi)$ for which $\varepsilon_C = \varepsilon_Q$, does there always exist a perturbed game $G' = (f,\pi')$ which is arbitrarily close to G (in some appropriate distance measure) for which a quantum advantage does exist? We do not have a general characterization of the games for which this is true, but we end with an example. Consider the game $G^M_{AND} = (f,\pi)$ where f is the 2-bit nonlocal AND function given by (5) and where $\pi(x,y) = (1/136)M_{xy}$, where the matrix M is the 4×4 magic square:

$$M = \begin{bmatrix} 4 & 14 & 15 & 1 \\ 9 & 7 & 6 & 12 \\ 5 & 11 & 10 & 8 \\ 16 & 2 & 3 & 13 \end{bmatrix}. \tag{12}$$

Exhaustive search over all classical strategies shows that $\varepsilon_C(G^M_{AND}) = 1/2$. On the other hand, using semidefinite programming (e.g. using the Matlab packages SeDuMi[12] and YALMIP [13]), it follows that $\varepsilon_Q(G^M_{AND}) \geq 0.5911$. This is interesting because the marginal distributions $\pi(x) = \sum_y \pi(x,y)$ and $\pi(y) = \sum_x \pi(x,y)$ are identical to the marginals of the game G_{AND}, for which no quantum advantage exists. In both cases, the two marginals (which correspond to the marginal probabilities that Alice and Bob receive strings x and y respectively) are equal to 1/4, independent of x and y. So this game is locally indistinguishable to Alice and Bob from G_{AND}, and yet a quantum advantage exists for G^M_{AND}. It would be interesting to know, for instance, whether it is possible to have a game where the marginals are random but the quantum value is equal to that of the CHSH game.

We thank M. van den Berg, T. Cubitt, T. Lawson and J. Sharam for helpful conversations. We gratefully acknowledge support for this work from: the Dorothy Hodgkin Foundation [JA]; the NWO Vici-project 639.023.302 and BRICKS project AFM1 [HB], the UK EPSRC through the QIP-IRC and the University of Bristol for a Research Fellowship [NL]; the EU project QAP [HB and NL].

* Electronic address: jon.allcock@bristol.ac.uk

[1] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[3] C. Bennett and S. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[4] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).
[5] R. de Wolf, Theor. Comp. Science **287**, 337 (2002).
[6] J. Clauser, M. Horne, A. Shimony, and R. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[7] N. Linden, S. Popescu, A. Short, and A. Winter, Phys. Rev. Lett. **99**, 180502 (2007).
[8] G. Brassard, H. Buhrman, N. Linden, A. Méthot, A. Tapp, and F. Unger, Phys. Rev. Lett. **96**, 250401 (2006).
[9] R. Cleve, P. Hoyer, B. Toner, and J. Watrous, 19th Annual IEEE Conference on Computational Complexity p. 236 (2004).
[10] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay, Computational Complexity **17**, 282 (2008).

[11] N. Alon and A. Naor, Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing (2004).

[12] J. Sturm, Optimization Methods for Software **11**, 625 (1999).

[13] J. Lofberg, Proceedings of the CACSD Conference, Taipei, Taiwan (2004).